

SYSTEM AND METHOD FOR INTRUSION PREVENTION IN A COMMUNICATIONS NETWORK

Abstract of Disclosure

A method, system and program for preventing intrusion in a communications network. A source node initiates a request for network services, such as session establishment, database access, or application access. Known network resources and authorized user information is stored in a database at a network portal along with access policy rules that are device and user dependent. Identification of the source node is required before the source node can construct a transformed packet header that is included with a synchronization packet before transmission to a destination node. An appliance or firewall in the communications network receives and authenticates the synchronization packet before releasing the packet to its intended destination. The authentication process includes verification of the access policy associated with the source node. Once received at the destination node, the transformed packet header is reformed by extracting a key index value. The extracted key index is subsequently used to transform the packet header in the response transmitted to the source node.

Figures